Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON A SPECIAL CLASS OF ABELIAN GROUPS.

BY G. A. MILLER.

1. Let $s_1, s_2, \ldots, s_{g_1}$ represent the $\phi(g)$* natural numbers which are less than g and prime to it. These g_1 numbers constitute a group (G_1) with respect to multiplication if the smallest positive residues mod g are taken in place of the products; for, from the relation $s_i s_h = qg + r$, $0 < r < g$, it follows that, if g and r had a common divisor, a prime factor of this divisor would have to divide either s_i or s_h, and thus these numbers would not both be prime to g. The other necessary conditions for a group are evidently satisfied. Such groups have recently received considerable attention, and, in the second edition of his Algebra, Weber† has called them the most important example of abelian groups of finite order. The main objects of this paper are to show that all these groups are groups of isomorphisms of the cyclical groups and to study some of their special properties.

2. By the *group of isomorphisms* of a given group G' whose elements (operators) are $t_1, t_2, \ldots, t_{g'}$ is meant the following group. Let G' be simply isomorphic with itself, the element t_i corresponding to $t_{\omega(i)}$, and form the substitution

$$J = \begin{pmatrix} t_1 & t_2 & \ldots & t_{(g')} \\ t_{\omega(1)} & t_{\omega(2)} & \ldots & t_{\omega(g')} \end{pmatrix}$$

Then the totality of such substitutions constitutes a group‡ and this is the group in question. The following considerations lead to the group of isomorphisms of a group generated by a single element S. Let T be any element that satisfies the equation $T^{-1}ST = S^{\alpha}$. Raising both members of this equation to the βth power we have $T^{-1}S^{\beta}T = S^{\alpha\beta}$. We may express this well known result in words as follows: If an element transforms a generator of a cyclical group into a given power, it transforms each one of the elements of this cyclical group into the same power.

---

* *Cf.* Chrystal's *Algebra*, vol. 2, 1889, p. 511.

† Weber, *Lehrbuch der Algebra*, 2d ed., vol. 2, 1899, p. 60.

‡ Hölder, *Math. Annalen*, vol. 43 (1893), p. 314. *Cf.* Moore, *Bull. Amer. Math. Soc.* vol. 1 (1894), p. 61.

In any holomorphism of a cyclical group G of order g with itself the $\phi(g)$ elements of order g must correspond to each other. A given generator S must therefore correspond to S^k, where k is prime to g. Since any holomorphism of a group with itself can be obtained by transforming all the elements of the group by a single element* it follows from the preceding paragraph that such a holomorphism is obtained by making each element correspond to its kth power. This result follows also directly from the fact that in any holomorphism like powers of corresponding elements yield corresponding elements. Since k is prime to g we may assume that $k = s_\alpha$ $(0 < \alpha \leqq g_1)$ and that the $s_1, s_2, \ldots s_{g_1}$ powers of S correspond to the $s_\alpha s_1, s_\alpha s_2, \ldots, s_\alpha s_{g_1}$ powers respectively in the given holomorphism of G with itself. Hence any holomorphism of G with itself corresponds to a substitution of the form

$$J_\alpha = \begin{pmatrix} s_1, & s_2, & \ldots\ldots & s_{g_1} \\ s_\alpha s_1, & s_\alpha s_2, & \ldots\ldots & s_\alpha s_{g_1} \end{pmatrix} \bmod g$$

and for every substitution of this form there is a holomorphism of G with itself. That is, the totality of these substitutions constitutes the group of isomorphisms of G. This group is obviously holomorphic with the group $s_1, s_2, \ldots, s_{g_1}$.

Thus the first of the two objects mentioned above is attained, viz. it is proved that the group G_1, whose elements are the $\phi(g)$ numbers that are less than g and prime to it, is the group of isomorphisms of the cyclical group of order g. This connects explicitly Burnside's study of the groups of isomorphisms of cyclical groups† and Weber's treatment of such groups as G_1.‡ In what follows we aim to establish a few properties of these groups which do not seem to have been explicitly noticed.

3. While the group of isomorphisms of a cyclical group is always abelian we shall prove that there are many abelian groups which cannot be the groups of isomorphisms of cyclical groups. Hence the groups which can be represented in the same manner as G_1 is represented above constitute a special class of abelian groups. We proceed to consider some of the conditions that must be

---

* Frobenius, *Berliner Sitzungsberichte*, 1895, p. 184.

† Burnside, *Theory of Groups of a Finite Order*, 1897, p. 240.

‡ Weber, *l. c.*

satisfied in order that an abelian group (A) may belong to this class. When (A) is cyclical the matter is quite simple. It is necessary and sufficient that its order (a) is the exponent to which a primitive root of some number belongs. That is, whenever $a = p^a(p-1)$*, p being an odd prime number and a being any positive integer including 0, the cyclical group (A) belongs to the given class, and only then. The lowest two even numbers which are not of the form $p^a(p-1)$ are 8 and 14; hence these numbers are the lowest orders of cyclical groups of an even order that cannot be the groups of isomorphisms of any groups whatever.

If g is written in the form: $g = 2^{a_0} p_1^{a_1} p_2^{a_2} \ldots$ ($p_1, p_2 \ldots$ being different odd prime numbers) G is the direct product of its subgroups of orders $2^{a_0}, p_1^{a_1}, p_2^{a_2}, \ldots$ and G_1 is the direct product of the groups of isomorphisms of these subgroups.† Since the group of isomorphisms of a cyclical group whose order is a power of an odd prime number is cyclical, it follows from the above that G_1 is the direct product of the cyclical groups of orders $p_1^{a_1-1}(p_1-1)$, $p_2^{a_2-1}(p_2-1) \ldots$ when $a_0 = 0$ or 1. When $a_0 > 1$ we have to add a group of order 2 and a cyclical group of order 2^{a_0-2} to these factor groups in order to obtain G_1.‡

Since G_1 is the direct product of groups of even orders, g_1 *is always even*. It can clearly be any even number of the form $2^{\beta_0} p_2^{\beta_1} p_2^{\beta_2} \ldots . (p_1 - 1)(p_2 - 1) \ldots$ The smallest two natural numbers which are not of this form are 14 and 26§; hence these numbers are the lowest even orders of groups that cannot be groups of isomorphisms of any cyclical groups whatever. It is evident that the highest prime factor of g_1 cannot exceed the highest prime factor of g.

In conclusion I consider briefly the groups G_1 of order g_1, the power of a prime; this prime is then necessarily 2. Therefore g has the form: $g = 2^{a_0} p_1 p_2 \ldots$, where the odd primes (if any) are of the respective forms: $p_1 = 2^{\beta_1} + 1$, $p_2 = 2^{\beta_2} + 1, \ldots; \beta_1 < \beta_2 < \ldots .$ The group G_1 is then the direct product of cyclic groups of orders $2^{\beta_1}, 2^{\beta_2}, \ldots$, and further, if $a_0 > 1$, of cyclic groups of orders 2 and 2^{a_0-2}. These orders are the invariants of the abelian group G_1. They are all distinct except in the cases: (1°) $\beta_1 = 1$, $a_0 > 1$; (2°) $\beta_1 > 1$, $\beta_\gamma = a_0 - 2 > 1$; (3°) $a_0 - 2 = 1$. The necessary and sufficient condition that G_1 contains three equal invariants is that (1°) and (3°) are both satisfied; hence G_1 cannot contain three equal invariants unless each is two. When $\beta_1 = 1$ and $\beta_\gamma = \alpha_0 - 2 > 1$, G_1 contains two pairs of equal invariants. These are the only cases in which G_1 can contain more than one pair of equal invariants.

---

* *Cf.* Dirichlet-Dedekind, *Zahlentheorie*, 1879, p. 340.

† *Bull. Amer. Math. Soc.*, vol. 5 (1899), p. 296.

‡ *Cf.* Burnside, *l. c.*

§ Lucas, *Théorie des nombres*, 1891, p. 394.

Cornell University, April 1900.